We claim:

1. A system for providing a provable chain of evidence for an evidence collection, comprising:

a security core which provides security functions;

one or more components;

means for operating the security core;

means for securely operably connecting the components to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

means for recording one or more data streams which comprise the evidence collection, each of the data streams being created by selected ones of the securely operably connected components; and

means for securely providing, for the evidence collection by the security core, an identification of each of the selected ones which create the recorded data streams.

2. The system according to Claim 1, wherein selected ones of the operable connections are made using one or more buses of the security core.

3. The system according to Claim 1, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

4. The system according to Claim 3, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

5. The system according to Claim 1, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

6. The system according to Claim 1, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

7. The system according to Claim 1, wherein the means for securely operably connecting further comprises means for authenticating the operably connected component to the security core.

8. The system according to Claim 7, wherein the means for authenticating further comprises:

means for providing a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and

means for using, by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

9. The system according to Claim 1, wherein the means for securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

10. The system according to Claim 7, wherein the means for authenticating are securely stored on the operably connected component.

11. The system according to Claim 7, further comprising means for authenticating the security core to the operably connected component.

12. The system according to Claim 1, further comprising means for authenticating a user involved in operating the security core and the operably connected components.

13. The system according to Claim 1, further comprising:

means for detecting whether the selected ones remain operably connected to the security core during operation of the means for recording; and

means for aborting the recording if one or more of the selected ones fails to remain operably connected to the security core during operation of the means for recording.

14. The system according to Claim 1, further comprising:

means for detecting whether the components remain operably connected to the security core during operation of the means for recording; and

means for marking the evidence collection as not authenticated if one or more of the components fails to remain operably connected to the security core during operation of the means for recording.

15. The system according to Claim 7, further comprising:

means for determining whether the selected ones have been authenticated to the security core; and

means for aborting the evidence collection if one or more of the selected ones has not been authenticated to the security core.

16. The system according to Claim 7, further comprising:

means for determining whether the selected ones have been authenticated to the security core; and

means for marking the evidence collection as not authenticated if one or more of the selected ones has not been authenticated to the security core.

17. The system according to Claim 7, further comprising:

means for determining whether the selected ones have been authenticated to the security core; and

means for suppressing from the evidence collection any data streams created by those ones of the selected ones that have not been authenticated to the security core.

18. The system according to Claim 1, wherein the means for securely providing further comprises means for digitally notarizing, by the security core, the recorded data streams which comprise the evidence collection.

19. The system according to Claim 1, wherein the means for securely providing further comprises means for adding another data stream to the evidence collection, wherein the added data stream comprises a digital notarization, created by the security core, of the recorded data streams which comprise the evidence collection.

20. The system according to Claim 18, wherein the means for digitally notarizing further comprises:

means for computing, by the security core, a hash value over each of the recorded data streams;

means for combining each hash value with a unique identifier of the selected one which created the recorded data stream for which the hash value was computed, thereby creating a combination data block;

means for hashing the combination data block;

means for digitally signing the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and

means for providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the recorded data streams which comprise the evidence collection, wherein the digital notarization cryptographically seals contents of the evidence collection and identities of the selected ones.

21. The system according to Claim 20, wherein:

the means for computing a hash operates periodically, upon expiration of an elapsed time value, to compute a hash value over each of a plurality of segments of each recorded data stream;

the means for combining, the means for hashing, and the means for digitally signing all operate on the periodically-computed hash values for each recorded data stream; and

the means for providing provides the digitally signed periodically-computed hash values, along with the periodically-computed hash values, as the digital notarization; and

further comprising means for inserting an identification of a time corresponding to each of the periodically-computed hash values at appropriate locations within each of the recorded data streams.

22. The system according to Claim 21, wherein the means for inserting uses MPEG-4 synchronization timestamping.

23. The system according to Claim 21, wherein authenticity and integrity of each of the segments is independently verifiable.

24. The system according to Claim 21, further comprising:

means for extracting selected ones of the segments of the recorded data streams; and

means for verifying integrity of the extracted selected ones using the public cryptographic key of the security core.

25. The system according to Claim 20, further comprising:

means for extracting selected ones of the recorded data streams; and

means for verifying authenticity of the extracted selected ones using the public cryptographic key of the security core.

26. The system according to Claim 19, further comprising:

means for authenticating a user involved in creating the recorded data streams; and

means for including an identification of the authenticated user in the digital notarization.

27. The system according to Claim 20, further comprising means for verifying authenticity of the evidence collection by a receiver of the recorded data streams and the digital notarization, using a public cryptographic key of the security core, wherein the public cryptographic key is cryptographically associated with a private cryptographic key that was used by the security core

to create the digital notarization, and for concluding that the evidence collection is authentic if the verification succeeds.

28. The system according to Claim 27, wherein the means for verifying authenticity further comprises concluding that the evidence collection has not been tampered with if the verification succeeds.

29. The system according to Claim 1, wherein the one or more recorded data streams of the evidence collection comprise an audio transcript.

30. The system according to Claim 29, wherein the evidence collection further comprises an identification of participants who are speaking in the audio transcript, wherein identification of the participants is provided by one of the selected ones.

31. The system according to Claim 1, wherein at least one of the one or more recorded data streams of the evidence collection comprises video data.

32. The system according to Claim 1, wherein the one or more recorded data streams of the evidence collection comprise a photograph and identifying information pertaining to taking the photograph.

33. The system according to Claim 32, wherein the identifying information further comprises at least one of: (1) a time of day when the photograph was taken; (2) a date when the photograph was taken; (3) a location where the photograph was taken, (4) a direction of the camera when the photograph was taken; and (5) settings of the camera when the photograph was taken; wherein the time, date, and location are provided by one or more of the selected ones.

34. The system according to Claim 1, further comprising:

means for recording an audio transcript by a first selected one of the securely operably connected components;

means for converting the audio transcript to a digital data stream by a second selected one of the securely operably connected components;

means for digitally notarizing the digital data stream, by the security core;

means for using the digital data stream as the recorded data stream of the evidence collection; and

means for using the digital notarization as the securely provided identification.

35. The system according to Claim 34, wherein the means for digitally notarizing further comprise:

means for computing a hash of the digital data stream;

means for combining the hash and a unique identifier of each of the first selected one and the second selected one, thereby creating a data block;

means for hashing the data block; and

means for digitally signing the hash of the data block using a private cryptographic key of the security core.

36. The system according to Claim 33, wherein the location is provided by one of the selected ones which is a global positioning satellite receiver.

37. A method of creating a provable chain of evidence for an evidence collection, comprising steps of:

providing a security core which provides security functions;

securely operably connecting one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

recording one or more data streams which comprise the evidence collection, each of the data streams being created by selected ones of the securely operably connected components; and

securely providing, for the evidence collection by the security core, an identification of each of the selected ones which create the recorded data streams.

38. The method according to Claim 37, wherein selected ones of the operable connections are made using one or more buses of the security core.

39. The method according to Claim 37, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

40. The method according to Claim 39, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

41. The method according to Claim 37, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

42. The method according to Claim 37, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

43. The system according to Claim 37, wherein the step of securely operably connecting further comprises the step of authenticating the operably connected component to the security core.

44. The method according to Claim 43, wherein the authenticating step further comprises the steps of:

providing a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and

using, by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

45. The method according to Claim 37, wherein the step of securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

46. The method according to Claim 43, wherein instructions for performing the authenticating step are securely stored on the operably connected component.

47. The method according to Claim 43, further comprising the step of authenticating the security core to the operably connected component.

48. The method according to Claim 37, further comprising the step of authenticating a user involved in operating the security core and the operably connected components.

49. The method according to Claim 37, further comprising steps of:

detecting whether the components remain operably connected to the security core during operation of the recording step; and

aborting the recording if one or more of the components fails to remain operably connected to the security core during operation of the recording step.

50. The method according to Claim 37, further comprising steps of:

detecting whether the selected ones remain operably connected to the security core during operation of the recording step; and

marking the evidence collection as not authenticated if one or more of the selected ones fails to remain operably connected to the security core during operation of the recording step.

51. The method according to Claim 43, further comprising steps of:

determining whether the selected ones have been authenticated to the security core; and

aborting the evidence collection if one or more of the selected ones has not been authenticated to the security core.

52. The method according to Claim 43, further comprising steps of:

determining whether the selected ones have been authenticated to the security core; and

marking the evidence collection as not authenticated if one or more of the selected ones has not been authenticated to the security core.

53. The method according to Claim 43, further comprising steps of:

determining whether the selected ones have been authenticated to the security core; and

suppressing from the evidence collection any data streams created by those ones of the selected ones that have not been authenticated to the security core.

54. The method according to Claim 37, wherein the step of securely providing further comprises the step of digitally notarizing, by the security core, the recorded data streams which comprise the evidence collection.

55. The method according to Claim 37, wherein the step of securely providing further comprises the step of adding another data stream to the evidence collection, wherein the added data stream comprises a digital notarization, created by the security core, of the recorded data streams which comprise the evidence collection.

56. The method according to Claim 54, wherein the digitally notarizing step further comprises steps of:

computing, by the security core, a hash value over each of the recorded data streams;

combining each hash value with a unique identifier of the selected one which created the recorded data stream for which the hash value was computed, thereby creating a combination data block;

hashing the combination data block;

digitally signing the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and

providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the recorded data streams which comprise the evidence

collection, wherein the digital notarization cryptographically seals contents of the evidence collection and identities of the selected ones.

57. The method according to Claim 56, wherein:

the step of computing a hash operates periodically, upon expiration of an elapsed time value, to compute a hash value over each of a plurality of segments of each recorded data stream;

the combining step, the hashing step, and the digitally signing step all operate on the periodically-computed hash values for each recorded data stream; and

the providing step provides the digitally signed periodically-computed hash values, along with the periodically-computed hash values, as the digital notarization; and

further comprising the step of inserting an identification of a time corresponding to each of the periodically-computed hash values at appropriate locations within each of the recorded data streams.

58. The method according to Claim 57, wherein the inserting step uses MPEG-4 synchronization timestamping.

59. The method according to Claim 57, wherein authenticity and integrity of each of the segments is independently verifiable.

60. The method according to Claim 57, further comprising steps of:

extracting selected ones of the segments of the recorded data streams; and

verifying integrity of the extracted selected ones using the public cryptographic key of the security core.

61. The method according to Claim 56, further comprising steps of:

extracting selected ones of the recorded data streams; and

verifying authenticity of the extracted selected ones using the public cryptographic key of the security core.

62. The method according to Claim 55, further comprising steps of:

authenticating a user involved in creating the recorded data streams; and

including an identification of the authenticated user in the digital notarization.

63. The method according to Claim 56, further comprising the step of verifying authenticity of the evidence collection by a receiver of the recorded data streams and the digital notarization, using a public cryptographic key of the security core, wherein the public cryptographic key is cryptographically associated with a private cryptographic key that was used by the security core to create the digital notarization, and concluding that the evidence collection is authentic if the verification succeeds.

64. The method according to Claim 63, wherein the step of verifying authenticity further comprises concluding that the evidence collection has not been tampered with if the verification succeeds.

65. The method according to Claim 37, wherein the one or more recorded data streams of the evidence collection comprise an audio transcript.

66. The method according to Claim 65, wherein the evidence collection further comprises an identification of participants who are speaking in the audio transcript, wherein identification of the participants is provided by one of the selected ones.

67. The method according to Claim 37, wherein at least one of the one or more recorded data streams of the evidence collection comprises video data.

68. The method according to Claim 37, wherein the one or more recorded data streams of the evidence collection comprise a photograph and identifying information pertaining to taking the photograph.

69. The method according to Claim 68, wherein the identifying information further comprises at least one of: (1) a time of day when the photograph was taken; (2) a date when the photograph was taken; (3) a location where the photograph was taken; (4) a direction of the camera when the photograph was taken; and (5) settings of the camera when the photograph was taken; wherein the time, date, and location are provided by one or more of the selected ones.

70. The method according to Claim 37, further comprising steps of:

recording an audio transcript by a first selected one of the securely operably connected components;

converting the audio transcript to a digital data stream by a second selected one of the securely operably connected components;

digitally notarizing the digital data stream, by the security core;

using the digital data stream as the recorded data stream of the evidence collection; and

using the digital notarization as the securely provided identification.

71. The method according to Claim 70, wherein the digitally notarizing step further comprises steps of:

computing a hash of the digital data stream;

combining the hash and a unique identifier of each of the first selected one and the second selected one, thereby creating a data block;

hashing the data block; and

digitally signing the hash of the data block using a private cryptographic key of the security core.

72. The method according to Claim 69, wherein the location is provided by one of the selected ones which is a global positioning satellite receiver.

73. A computer program product for providing a provable chain of evidence for an evidence collection, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for operating a security core which provides security functions;

computer-readable program code means for securely operably connecting one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

computer-readable program code means for recording one or more data streams which comprise the evidence collection, each of the data streams being created by selected ones of the securely operably connected components; and

computer-readable program code means for securely providing, for the evidence collection by the security core, an identification of each of the selected ones which create the recorded data streams.

74. The computer program product according to Claim 73, wherein selected ones of the operable connections are made using one or more buses of the security core.

75. The computer program product according to Claim 73, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

76. The computer program product according to Claim 75, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

77. The computer program product according to Claim 73, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

78. The computer program product according to Claim 73, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

79. The computer program product according to Claim 73, wherein the computer-readable program code means for securely operably connecting further comprises computer-readable program code means for authenticating the operably connected component to the security core.

80. The computer program product according to Claim 79, wherein the computer-readable program code means for authenticating further comprises:

computer-readable program code means for providing a unique identifier of the operably connected component to the security core, along with a digital signature of the unique identifier that is created using a private key of the operably connected component; and

computer-readable program code means for using, by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component.

81. The computer program product according to Claim 73, wherein the computer-readable program code means for securely operably connecting is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

82. The computer program product according to Claim 79, wherein the computer-readable program code means for authenticating are securely stored on the operably connected component.

83. The computer program product according to Claim 79, further comprising computer-readable program code means for authenticating the security core to the operably connected component.

84. The computer program product according to Claim 73, further comprising computer-readable program code means for authenticating a user involved in operating the security core and the operably connected components.

85. The computer program product according to Claim 73, further comprising:

computer-readable program code means for detecting whether the selected ones remain operably connected to the security core during operation of the computer-readable program code means for recording; and

computer-readable program code means for aborting the recording if one or more of the selected ones fails to remain operably connected to the security core during operation of the computer-readable program code means for recording.

86. The computer program product according to Claim 73, further comprising:

computer-readable program code means for detecting whether the components remain operably connected to the security core during operation of the computer-readable program code means for recording; and

computer-readable program code means for marking the evidence collection as not authenticated if one or more of the components fails to remain operably connected to the security core during operation of the computer-readable program code means for recording.

87. The computer program product according to Claim 79, further comprising:

computer-readable program code means for determining whether the selected ones have been authenticated to the security core; and

computer-readable program code means for aborting the evidence collection if one or more of the selected ones has not been authenticated to the security core.

88. The computer program product according to Claim 79, further comprising:

computer-readable program code means for determining whether the selected ones have been authenticated to the security core; and

computer-readable program code means for marking the evidence collection as not authenticated if one or more of the selected ones has not been authenticated to the security core.

89. The computer program product according to Claim 79, further comprising:

computer-readable program code means for determining whether the selected ones have been authenticated to the security core; and

computer-readable program code means for suppressing from the evidence collection any data streams created by those ones of the selected ones that have not been authenticated to the security core.

90. The computer program product according to Claim 73, wherein the computer-readable program code means for securely providing further comprises computer-readable program code means for digitally notarizing, by the security core, the recorded data streams which comprise the evidence collection.

91. The computer program product according to Claim 73, wherein the computer-readable program code means for securely providing further comprises computer-readable program code means for adding another data stream to the evidence collection, wherein the added data stream comprises a digital notarization, created by the security core, of the recorded data streams which comprise the evidence collection.

92. The computer program product according to Claim 90, wherein the computer-readable program code means for digitally notarizing further comprises:

computer-readable program code means for computing, by the security core, a hash value over each of the recorded data streams;

computer-readable program code means for combining each hash value with a unique identifier of the selected one which created the recorded data stream for which the hash value was computed, thereby creating a combination data block;

computer-readable program code means for hashing the combination data block;

computer-readable program code means for digitally signing the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and

computer-readable program code means for providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the recorded data streams which comprise the evidence collection, wherein the digital notarization cryptographically seals contents of the evidence collection and identities of the selected ones.

93. The computer program product according to Claim 92, wherein:

the computer-readable program code means for computing a hash operates periodically, upon expiration of an elapsed time value, to compute a hash value over each of a plurality of segments of each recorded data stream;

the computer-readable program code means for combining, the computer-readable program code means for hashing, and the computer-readable program code means for digitally signing all operate on the periodically-computed hash values for each recorded data stream; and

the computer-readable program code means for providing provides the digitally signed periodically-computed hash values, along with the periodically-computed hash values, as the digital notarization; and

further comprising computer-readable program code means for inserting an identification of a time corresponding to each of the periodically-computed hash values at appropriate locations within each of the recorded data streams.

94. The computer program product according to Claim 93, wherein the computer-readable program code means for inserting uses MPEG-4 synchronization timestamping.

95. The computer program product according to Claim 93, wherein authenticity and integrity of each of the segments is independently verifiable.

96. The computer program product according to Claim 93, further comprising:

computer-readable program code means for extracting selected ones of the segments of the recorded data streams; and

computer-readable program code means for verifying integrity of the extracted selected ones using the public cryptographic key of the security core.

97. The computer program product according to Claim 92, further comprising:

computer-readable program code means for extracting selected ones of the recorded data streams; and

computer-readable program code means for verifying authenticity of the extracted selected ones using the public cryptographic key of the security core.

98. The computer program product according to Claim 91, further comprising:

computer-readable program code means for authenticating a user involved in creating the recorded data streams; and

computer-readable program code means for including an identification of the authenticated user in the digital notarization.

99. The computer program product according to Claim 92, further comprising computer-readable program code means for verifying authenticity of the evidence collection by a receiver of the recorded data streams and the digital notarization, using a public cryptographic key of the security core, wherein the public cryptographic key is cryptographically associated with a private cryptographic key that was used by the security core to create the digital notarization, and for concluding that the evidence collection is authentic if the verification succeeds.

100. The computer program product according to Claim 99, wherein the computer-readable program code means for verifying authenticity further comprises concluding that the evidence collection has not been tampered with if the verification succeeds.

101. The computer program product according to Claim 73, wherein the one or more recorded data streams of the evidence collection comprise an audio transcript.

102. The computer program product according to Claim 101, wherein the evidence collection further comprises an identification of participants who are speaking in the audio transcript, wherein identification of the participants is provided by one of the selected ones.

103. The computer program product according to Claim 73, wherein at least one of the one or more recorded data streams of the evidence collection comprises video data.

104. The computer program product according to Claim 73, wherein the one or more recorded data streams of the evidence collection comprise a photograph and identifying information pertaining to taking the photograph.

105. The computer program product according to Claim 104, wherein the identifying information further comprises at least one of: (1) a time of day when the photograph was taken; (2) a date when the photograph was taken; (3) a location where the photograph was taken;(4) a direction of the camera when the photograph was taken; and (5) settings of the camera when the photograph was taken; wherein the time, date, and location are provided by one or more of the selected ones.

106. The computer program product according to Claim 73, further comprising:

computer-readable program code means for recording an audio transcript by a first selected one of the securely operably connected components;

computer-readable program code means for converting the audio transcript to a digital data stream by a second selected one of the securely operably connected components;

computer-readable program code means for digitally notarizing the digital data stream, by the security core;

computer-readable program code means for using the digital data stream as the recorded data stream of the evidence collection; and

computer-readable program code means for using the digital notarization as the securely provided identification.

107. The computer program product according to Claim 106, wherein the computer-readable program code means for digitally notarizing further comprise:

computer-readable program code means for computing a hash of the digital data stream;

computer-readable program code means for combining the hash and a unique identifier of each of the first selected one and the second selected one, thereby creating a data block;

computer-readable program code means for hashing the data block; and

computer-readable program code means for digitally signing the hash of the data block using a private cryptographic key of the security core.

108. The computer program product according to Claim 105, wherein the location is provided by one of the selected ones which is a global positioning satellite receiver.

109. A method of doing business by creating a provable chain of evidence for an evidence collection, comprising steps of:

operating a security core which provides security functions;

securely operably connecting one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component;

authenticating selected ones of the components to the security core, thereby securely operably connecting the selected ones, using a unique identifier of each selected one along with a digital signature of the unique identifier that is created using a private key of the selected one and using, by the security core, a public key that is cryptographically associated with the private key to determine authenticity of the operably connected component;

recording one or more data streams which comprise the evidence collection, the data streams being created by at least one of the selected ones; and

digitally notarizing, by the security core, the recorded data streams which comprise the evidence collection.

110. The method according to Claim 109, wherein the digitally notarizing step further comprises steps of:

computing, by the security core, a hash value over each of the recorded data streams;

combining each hash value with a unique identifier of the selected one which created the recorded data stream for which the hash value was computed, thereby creating a combination data block;

hashing the combination data block;

digitally signing the hashed combination data block with a private cryptographic key of the security core, wherein the private cryptographic key has a public cryptographic key cryptographically associated therewith; and

providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the recorded data streams which comprise the evidence collection, wherein the digital notarization cryptographically seals contents of the evidence collection and identities of the selected ones which created the recorded data streams of the evidence collection.